Table of Contents

Security Policies

Acceptable Use Statement

This document gives the requirements for use of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center.

As a user of the computing systems, resources and facilities located at and/or operated by the NASA Advanced Supercomputing (NAS) Division at NASA Ames Research Center, I agree to the following and understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution:

1. NAS accounts are to be used only for the purpose for which they are authorized and are not to be used for non-NASA related activities.
2. Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law (Section 799, Title 18, U.S. Code). I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that sharing passwords with other people, even on the same project, is prohibited. I understand that my misuse of assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of these systems
3. I am responsible for using the computing systems, resources and facilities in an efficient and effective manner. I understand that account deactivation will result after 60 days of non-use and data will be deleted after 90 days unless my project or I make arrangements with the NAS User Services to preserve my data.
4. I understand that these computing systems are unclassified systems. Therefore, processing and storing classified, or other information that requires safeguarding in the interest of National Security, is prohibited.
5. I understand that these computing systems are categorized as moderate according to FIPS 199, therefore processing and storing information that is categorized as high according to FIPS 199 and NIST SP 800-60 is prohibited.
6. I understand that I am responsible for protecting any information processed or stored in my accounts and will take appropriate precautions to protect Sensitive But Unclassified information (e.g., proprietary information or information subject to International Traffic in Arms Regulations or Export Control Regulations), which may include encrypting the data to provide protection that goes beyond the standard OS protection provided by the computing systems.
7. I understand that I shall not engage in activities that compromise or weaken the security of the NAS systems or have been identified as prohibited and high-risk practices by the NAS Security Team. These activities include but are not limited to

keeping unauthorized world-writable directories, running password cracking programs, downloading or introducing malicious software, running unauthorized P2P and VOIP software and copying or making available system and password configuration files to others.

8. I understand that I shall not make copies of copyrighted software, except as permitted by law or by the owner of the copyright.
9. I understand that I shall not attempt to access any data or programs contained on systems for which I do not have authorization or explicit consent from the owner of the data/program, the NAS Division Chief or the NAS Computer Security Official.
10. I understand that I am required to report any security weaknesses in the systems or any IT security incidents including misuse or violation of this agreement, to the NAS User Services, support@nas.nasa.gov, or to the NAS Security Team, security@nas.nasa.gov.
11. I understand that I am required to access the NAS Computers only from remote systems which are fire walled and are running regularly updated virus protection software.
12. I understand that I will be required to complete the NASA mandatory Basic IT Security Training available at: http://satern.nasa.gov/. (Note: Additional details are available from NAS User Services.)
13. If applicable, I further agree to abide by the provisions NASA NPD 2540.1F regulating privileges and responsibilities of NASA employees and contractors.

Account Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

Users are responsible for being aware of the general account-related policies below.

- Both users and NAS staff requesting either a new or a renewed account must complete the Basic IT security training **annually** and fill out an Account Request form for the annual NOP (new operational period).
- Users shall not share their account(s) with anyone. This includes sharing the password to the account, providing access via an .rhost entry or other means of sharing.
- Users are responsible for protecting any information used and/or stored on/in their accounts.

Account Deactivation

Users who do not comply with the rules listed in the Acceptable Use Statement will have their accounts disabled either temporarily or permanently. Account deactivation will result after 90 days of non-use (by changing user's normal shell to noshell) and data may be archived after 120 days of non-use.

Two-Factor Authentication and Policy

DRAFT

This article is being reviewed for completeness and technical accuracy.

What is two-factor authentication?

In the field of security, there are three general ways you can prove you are who you claim to be. Each way is called a "factor." The factors fall into the categories of (1) something you have, such as an ATM card, (2) something you know, such as the personal pin to your bank account, and (3) something you are, such as your fingerprint. Two-factor authentication refers to using any two of these factors to authenticate a person before access to systems is granted.

NAS Policy

At NAS, the three different factors used are:

1. your assigned RSA SecurID fob (sometimes called a key fob or a token)
2. your password to the NAS systems
3. your public/private key pair

You are required to authenticate yourself with two of these factors before you can access NAS resources from outside the NAS HECC Enclave. One of these two factors has to be the possession of your SecurID fob. Thus, you can authenticate yourself with a combination of either SecurID + password, or SecurID + public/private key pair.

Two-factor authentication is required when accessing

- the secure front-end systems, SFE1 and SFE2, from your local desktop systems
- any system inside the NAS HECC Enclave (such as Pleiades or Columbia) from your localhost using SSH Pasthrough.
- Bouncer or Bruiser (bastion hosts to other NAS desktop systems) from your local desktop systems
- Return to Flight (RTF) hosts through the web

Related articles: RSA SecurID Fob, Passwords, Public/Private Key Pairs

Password Creation Rules

DRAFT

This article is being reviewed for completeness and technical accuracy.

Your password is vulnerable to attack since it can be guessed. Follow the rules below when creating your NAS passwords:

1. Never use a password at NAS that has ever been used by you anywhere else, and never use the password that you create for NAS anywhere else, ever.

2. A password must contain a minimum of 8 characters. It must contain one character each from at least three of the following character sets: uppercase letters, lowercase letters, numbers, and special characters.

3. Use non-trivial passwords; examples of "trivial" passwords that you may not use include but are not limited to:

    - your user ID
    - a dictionary word of any language or a dictionary word with numbers appended or prepended to it
    - a password either wholly or predominately composed of the following: user ID, owner name, birthdate, Social Security Number, family member or pet's name, name spelled backwards, or other personal information
    - a contractor name
    - a division or branch name
    - repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
    - the name of any automobile or sport team
    - the name of any vendor product or nickname for a product
4. A new password can not be any one of your last 24 passwords.

5. Once you are successful in changing a password, you have to wait at least 7 days to change it again.
6. Passwords must be changed every 90 days.

Never share your password with anyone. For more information, read Account Policies and the Acceptable Use Statement.

Password Information and Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

This article outlines the processes and rules for getting your default password and changing your password.

Obtaining Your Password

If you are a new user and don't know your default installation password for the NAS high-performance computing systems, please call the NAS Control Room at 1-800-331-USER (8737) or 1-650-604-4444.

If you already have an account on a NAS system, and you are approved to get an account on another machine, your password on the new machine is your current "lou" password. If you do not remember this password, a Control Room analyst will provide you with a new default password.

NOTE: Due to security requirements, you must provide the Control Room analysts with a) the correct answer to a security question that you have already submitted to NAS, or b) the analyst must be able reach you at the phone number listed on your account request form. If your phone number has changed due to office moves or reorganizations, your PI must contact the Control Room stating the reason for the change via phone or FAX. The FAX number is 650-604-1777. If your PI is unavailable, your branch chief or division chief may do this for you.
Once you have been given a default password, you will be prompted to change it once you log in to a NAS system.

Password Creation Rules

Your password is vulnerable to attack since it can be guessed. Follow the rules below when creating your NAS passwords:

1. Never use a password at NAS that has ever been used by you anywhere else, and never use the password that you create for NAS anywhere else, ever.

2. A password must contain a minimum of 12 characters. It must contain one character each from at least three of the following character sets: uppercase letters, lowercase letters, numbers, and special characters.

3. Use non-trivial passwords; examples of "trivial" passwords that you may not use include, but are not limited to:

    - your user ID
    - a dictionary word of any language or a dictionary word with numbers appended or prepended to it
    - a password either wholly or predominately composed of the following: user ID, owner name, birthdate, Social Security Number, family member or pet's name, name spelled backwards, or other personal information
    - a contractor name
    - a division or branch name
    - repetitive or keyboard patterns (for example, "abc#ABC", "1234", "qwer", "mnbvc", "aaa#aaaa")
    - the name of any automobile or sport team
    - the name of any vendor product or nickname for a product
4. A new password cannot be any of your last 24 passwords.

5. Once you are successful in changing a password, you have to wait at least 7 days to change it again.
6. Passwords must be changed every 60 days.

Never share your password with anyone. For more information, see Account Policies and the Acceptable Use Statement.

ITAR/Export Control

DRAFT

This article is being reviewed for completeness and technical accuracy.

The PI must, by law, manage, protect and control the export of the project's data in a way that complies with the security category of the data. There are five categories of data:

- Mission Information (MSN)
- Business and Restricted Technology Information (BRT)
- Scientific, Engineering, and Research Information (SER)
- Administrative Information (ADM)
- Public Access Information (PUB)

```
Mission Information requires the most stringent security control
and protection. Currently, the NAS Facility is not configured to
provide services for MSN data. For Business and Restricted
Technology Information (which includes ITAR/Export Control Data),
no world access (write/read/execute) is allowed.
```

Detailed descriptions of each data categories are as follows:

Mission Information (MSN)

If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission. Examples in this category are those that control or directly support one of the following:

1. Human space flight
2. Wide Area Networks
3. Development of the data or software used to control human flight
4. Training simulation vehicles
5. Wind tunnel operations
6. Launch operations
7. Space vehicle operations

Business and Restricted Technology Information (BRT)

This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to our employees, in loss of business

for our partners and customer businesses, in contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws. Examples in this category are those that are related to the following kinds of information:

1. Financial
2. Legal
3. Payroll
4. Personnel
5. Procurement
6. Source selection
7. Proprietary information entrusted to the Government
8. Export controlled technical information (includes disclosure to foreign nationals)

Scientific, Engineering, and Research Information (SER)

All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category consists of information that supports basic research, engineering, and technology development but is less restricted against public disclosure.

1. Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the Agency in accomplishing a primary mission.
2. Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from such things as premature disclosure of their work by another party. The impact, however, is primarily on an individual rather than on the Agency.

Administrative Information (ADM)

Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, predecisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications-from problem reports to configuration management tools-on administrative IT systems.

1. This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting.
2. Integrity and availability are the driving IT security concerns. The impact is primarily managerial in nature, which would require time and resources to correct. Confidentiality may be of concern in certain specific administrative information. In

such instances, additional security controls must be imposed as a risk analysis dictates.

Public Access Information (PUB)

This category includes information, software applications, and computer systems specifically intended for public use or disclosure, such as a public web site or hands-on demonstrations. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA's missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

1. Information posted for public access which could expose NASA missions to risk if compromised should be afforded additional protective measures. In these cases, the baseline requirements for ADM information should be implemented. (For example, contractors may submit proposals based on information from NASA web sites. Loss, alteration, or unavailability of data at the site could result in protests, thereby impacting procurement cycle time and ultimately NASA missions.)
2. Integrity and availability are the driving concerns. IT security controls are selected to protect the resources themselves and are not intended to protect the confidentiality of the information.

Files and Directories Permissions Policies

DRAFT

This article is being reviewed for completeness and technical accuracy.

Write permission is granted only to the file owner. That is, files and directories may not be writable by group and/or others unless there is a valid justification. By default, files and directories are set with owner permissions.

To request write permissions for members of your group or others, your principal investigator (PI) must submit a valid justification by calling 1-800-331-USER or 1-650-604-4444, or by sending an e-mail to support@nas.nasa.gov. The request will be reviewed by the NAS security officer.

For directories, if a world write permission is approved by the security officer, the "sticky bit" must be set also (chmod +t) on that directory to prevent an unprivileged user from deleting or renaming files of other users in that directory.

File and directory permissions are routinely scanned for violation of this policy. For those files/directories that are permitted by the security officer to be writable by group and/or others, they will be recorded on an exception list.

SUID/SGID Scripts

DRAFT

This article is being reviewed for completeness and technical accuracy.

Users are prohibited from creating and using privileged SUID and/or SGID scripts under their home, scratch, nobackup and /tmp filesystems.

SUID scripts (that is, with permission u+s) and SGID scripts (with permission g+s) could allow someone (other than the owner) to gain unauthorized access to users' files, posing a security hazard.

The high end computing systems at the NAS facility are configured to disable the execution of any SUID/SGID shell scripts.